Attorney Docket No. 1083.1101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Eiji HASEGAWA, et al.

Application No.: Group Art Unit:

Filed: February 24, 2004 Examiner:

For: INFORMATION PROCESSING APPARATUS

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-372374

Filed: October 31, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 24, 2004 By: _____

J. Randall Beckers
Registration No. 30,358

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月３１日

出願番号
Application Number: 特願２００３－３７２３７４

[ST. 10/C]: [ＪＰ２００３－３７２３７４]

出願人
Applicant(s): 富士通株式会社

２００４年　２月１６日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００９６７８

【書類名】　特許願
【整理番号】　0395318
【提出日】　平成15年10月31日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F　9/06
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　長谷川　英司
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　本田　文雄
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100078868
　【弁理士】
　【氏名又は名称】　河野　登夫
　【電話番号】　06-6944-4141
【国等の委託研究の成果に係る記載事項】　平成１５年度、通信・放送機構、「ＰＣなどオープンアーキテクチャーデジタル放送受信機に対応する権利保護システムの研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受ける特許出願
【手数料の表示】
　【予納台帳番号】　001889
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9705356

【書類名】特許請求の範囲
【請求項１】
第１の記憶手段と、
該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、
セキュアモジュールと、
暗号化されたプログラムを記憶する第２の記憶手段と
を有する情報処理装置において、
前記第２の記憶手段は、複数に分割されたプログラムを記憶してあり、
前記ＣＰＵは、前記第２の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくなしてあり、
前記セキュアモジュールは、前記第２の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行されたプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。
【請求項２】
前記セキュアモジュールは、分割されたプログラムに対する実行要求信号を受信したか否かを判断する手段を備え、該手段が実行要求信号を受信したと判断した場合、受け取ったプログラムを実行可能な状態へ復帰させるものであることを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記セキュアモジュールは、分割されたプログラムについて、前記第１の記憶手段にプログラム実行前に常駐させるプログラムか、実行されるまで前記メモリに書き込まれないプログラムかを識別する情報を記憶する手段を備えることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
第１の記憶手段と、
該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、
セキュアモジュールと、
暗号化されたプログラムを記憶する第２の記憶手段と
を有する情報処理装置において、
前記ＣＰＵは、前記第２の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくなしてあり、
前記セキュアモジュールは、前記第２の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを複数に分割する手段と、分割されたプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行されたプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。
【請求項５】
前記第２の記憶手段は、記憶されたプログラムに対応付けて、プログラムの分割に関する情報を記憶してあり、前記セキュアモジュールは、前記プログラムの分割に関する情報に基づいて受け取ったプログラムを複数に分割すべくなしてあることを特徴とする請求項４記載の情報処理装置。
【請求項６】
第１の記憶手段と、
該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、
セキュアモジュールと、
暗号化されたプログラムを記憶する第２の記憶手段と
を有する情報処理装置において、

前記第１の記憶手段は、複数に分割されたプログラムを実行前に常駐させてあり、

前記第２の記憶手段は、分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを記憶してあり、前記第２の記憶手段に記憶された呼び出しプログラムを前記セキュアモジュールへ転送すべくなしてあり、

前記セキュアモジュールは、前記第２の記憶手段に記憶された呼び出しプログラムを受け取る手段と、受け取った呼び出しプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが分割されたプログラムを実行する順序で、対応する実行可能な状態へ復帰された呼び出しプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行された呼び出しプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする情報処理装置。

【請求項７】

前記第１の記憶手段は、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報をさらに記憶してあり、前記セキュアモジュールは、前記リンク情報に基づいて分割されたプログラムを実行する順序を検出すべくなしてあることを特徴とする請求項６記載の情報処理装置。

【書類名】明細書
【発明の名称】情報処理装置
【技術分野】
【０００１】
本発明は、プログラムを実行する場合に、悪意の第三者による解析を困難にする情報処理装置に関する。特に、情報処理装置に着脱可能に実装され、プログラムを実行する際のセキュリティに関する処理を実行するセキュアモジュールを用いた情報処理装置に関する。
【背景技術】
【０００２】
近年、ブロードバンドインターネットに代表される常時接続環境が普及し、悪意ある第三者による不正なプログラムの実行、更新等に対する安全性を確保する技術が着目されている。特に、パーソナルコンピュータ（Personal Computer：以下「ＰＣ」という。）はオープンなアーキテクチャを有し、ＰＣ上で実行されるプログラムは、オペレーティングシステム（以下、ＯＳという。）又はプロセッサに準拠した形式のプログラムコードとして記述される。したがって、基本的には誰でもＰＣ上のメインメモリの内容を確認し、理解することができるため、安全性を確保することは困難であるという問題点があった。
【０００３】
斯かる問題点を解決すべく、従来は、実行されるプログラムを難読化又はセキュア化する技術を使用し、例えばプログラムのロジックを複雑にすることにより逆解析を困難にする、プログラムを暗号化する、プログラムをメモリに動的に書き込みながら実行する（特許文献１参照）等の対策が取られている。
【０００４】
また、特許文献２には、オープンなアーキテクチャを有する情報処理装置に、外部モジュールとして、内部に解析又は参照することが不可能な領域を有するセキュアモジュールを組み合わせ、該セキュアモジュールによりプログラムをメモリに書き込む技術が開示されている。斯かる技術を用いる場合、プログラムが記憶媒体に記憶されている間は、外部から解析又は参照することが不可能な情報を使用してプログラムを暗号化しており、第三者による内容の解析を防止している。また、プログラムを書き込んだメモリをプロセッサと独立動作するセキュアモジュールにより監視することにより、実行するプログラムの安全性をより高めている。
【特許文献１】特開平１１－２３２１０３号公報
【特許文献２】特開２００３－１９８５２７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、実行されるプログラムを難読化又はセキュア化する技術を使用する方法では、いかにプログラムを難読化又はセキュア化しようと、最終的にはオープンなアーキテクチャ上で動作するプログラムとして記述することには変わりはない。したがって、メモリに書き込まれたロードモジュールを逆解析し、周知であるオープンなアーキテクチャに沿って命令、データ等を調査することで、実行されるプログラムの内容を解析することは可能であり、第三者による不正な攻撃を防ぐことはできない。
【０００６】
また、セキュアモジュールを用いてプログラムをメモリに書き込んで実行する方法を使用する場合であっても、プロセッサが実行可能な形式でプログラムがメモリに書き込まれることには変わりはなく、メモリの内容をイメージコピーし、イメージコピーに基づいてメモリの内容を解析することで、実行されるプログラムの内容を解析することは可能である。
【０００７】
本発明は斯かる事情に鑑みてなされたものであり、プログラムを実行する場合に、悪意

ある第三者による逆解析を困難にし、実行するプログラムの安全性を高めることができる情報処理装置を提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記目的を達成するために第１発明に係る情報処理装置は、第１の記憶手段と、該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、セキュアモジュールと、暗号化されたプログラムを記憶する第２の記憶手段とを有する情報処理装置において、前記第２の記憶手段は、複数に分割されたプログラムを記憶してあり、前記ＣＰＵは、前記第２の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくなしてあり、前記セキュアモジュールは、前記第２の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行されたプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする。

【０００９】

第１発明に係る情報処理装置では、暗号化されたプログラムを複数に分割して記憶しておき、分割されたプログラム単位で実行可能な状態へ復帰させ、実行する順序で第１の記憶手段（例えばメモリ）へ書き込む。実行が完了したプログラムは、第１の記憶手段上から削除する。これにより、プログラム実行時にプログラムのすべての内容が第１の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第１の記憶手段へ書き込まれていることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

【００１０】

また、第２発明に係る情報処理装置は、第１発明において、前記セキュアモジュールは、分割されたプログラムに対する実行要求信号を受信したか否かを判断する手段を備え、該手段が実行要求信号を受信したと判断した場合、受け取ったプログラムを実行可能な状態へ復帰させるものであることを特徴とする。

【００１１】

第２発明に係る情報処理装置では、分割されたプログラムに対する実行要求信号を受信してから、要求対象である分割されたプログラムを実行可能な状態へ復帰させて第１の記憶手段（例えばメモリ）へ書き込む。これにより、実行要求が出された時点で初めて第１の記憶手段へプログラムが記憶されることから、実行要求が出されるまではプログラムの一部は第１の記憶手段へ書き込まれておらず、外部から第１の記憶手段の内容を参照した場合であってもプログラム全体の内容を把握することは困難であり、実行するプログラムの安全性をより高めることが可能となる。

【００１２】

また、第３発明に係る情報処理装置は、第１発明又は第２発明において、前記セキュアモジュールは、分割されたプログラムについて、前記第１の記憶手段にプログラム実行前に常駐させるプログラムか、実行されるまで前記メモリに書き込まれないプログラムかを識別する情報を記憶する手段を備えることを特徴とする。

【００１３】

第３発明に係る情報処理装置では、分割されたプログラムの重要性、秘匿性等に基づいて、第１の記憶手段(例えばメモリ)に常時書き込んでおいてもよいプログラムであるか否かを識別する情報を付与する。これにより、重要性、秘匿性等の低いプログラムは第１の記憶手段上に常時書き込んでおき、重要性、秘匿性等の高いプログラムは実行時のみ第１の記憶手段に書き込むことで、必要なプログラムのみ実行の安全性を高めることができ、安全性を確保するための処理によるプログラムのオーバヘッドを低減することが可能となる。

【００１４】
また、第４発明に係る情報処理装置は、第１の記憶手段と、該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、セキュアモジュールと、暗号化されたプログラムを記憶する第２の記憶手段とを有する情報処理装置において、前記ＣＰＵは、前記第２の記憶手段に記憶されたプログラムを前記セキュアモジュールへ転送すべくなしてあり、前記セキュアモジュールは、前記第２の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを複数に分割する手段と、分割されたプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが実行する順序で、実行可能な状態へ復帰されたプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行されたプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする。
【００１５】
第４発明に係る情報処理装置では、セキュアモジュールが、記憶されている暗号化されたプログラムを複数に分割し、分割したプログラム単位で実行可能な状態へ復帰させ、実行する順序で第１の記憶手段（例えばメモリ）へ書き込む。実行が完了したプログラムは、第１の記憶手段上から削除する。これにより、プログラム実行時にプログラムのすべての内容が第１の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第１の記憶手段へ書き込まれていることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。
【００１６】
また、第５発明に係る情報処理装置は、第４発明において、前記第２の記憶手段は、記憶されたプログラムに対応付けて、プログラムの分割に関する情報を記憶してあり、前記セキュアモジュールは、前記プログラムの分割に関する情報に基づいて受け取ったプログラムを複数に分割すべくなしてあることを特徴とする。
【００１７】
第５発明に係る情報処理装置では、セキュアモジュールは、受け取る分割されたプログラムに対応付けて記憶されているプログラムの分割に関する情報、例えば分割単位に基づいてプログラムを分割し、分割したプログラム単位で実行可能な状態へ復帰させる。これにより、記憶されているプログラムの分割に関する情報に基づいて適正にプログラムを分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが第１の記憶手段に書き込まれる状態が生じることを回避し、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。
【００１８】
また、第６発明に係る情報処理装置は、第１の記憶手段と、該第１の記憶手段に書き込まれたプログラムを実行するＣＰＵと、セキュアモジュールと、暗号化されたプログラムを記憶する第２の記憶手段とを有する情報処理装置において、前記第１の記憶手段は、複数に分割されたプログラムを実行前に常駐させてあり、前記第２の記憶手段は、分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを記憶してあり、前記第２の記憶手段に記憶された呼び出しプログラムを前記セキュアモジュールへ転送すべくなしてあり、前記セキュアモジュールは、前記第２の記憶手段に記憶された呼び出しプログラムを受け取る手段と、受け取った呼び出しプログラムを実行可能な状態へ復帰させる手段と、前記ＣＰＵが分割されたプログラムを実行する順序で、対応する実行可能な状態へ復帰された呼び出しプログラムを前記第１の記憶手段に書き込む手段と、前記ＣＰＵにより実行された呼び出しプログラムを、実行終了後に前記第１の記憶手段から削除する手段とを備えることを特徴とする。
【００１９】
第６発明に係る情報処理装置では、暗号化されたプログラムを複数に分割し、分割され

たプログラム単位で実行可能な状態へ復帰させ、すべての分割されたプログラムを第１の記憶手段（例えばメモリ）へ書き込んでおく。そして、プログラム間のリンク手段でもある分割されたプログラムを実行プログラムとして呼び出す呼び出しプログラムを暗号化し、分割されたプログラムを実行する順序で呼び出しプログラムを実行可能な状態へ復帰させ、第１の記憶手段へ書き込む。実行が完了した呼び出しプログラムは、第１の記憶手段上から削除する。これにより、プログラム実行時に分割されたプログラムは第１の記憶手段上に書き込まれているが、分割されたプログラム間の関係が不明であることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、分割されたプログラムの実行順序、実行タイミング等を解析することが困難であり、実行するプログラムの安全性を確保することが可能となる。

【００２０】

また、第７発明に係る情報処理装置は、第６発明において、前記第１の記憶手段は、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報をさらに記憶してあり、前記セキュアモジュールは、前記リンク情報に基づいて分割されたプログラムを実行する順序を検出すべくなしてあることを特徴とする。

【００２１】

第７発明に係る情報処理装置では、分割されたプログラム間の呼び出し関係を指定する情報であるリンク情報に基づいて分割されたプログラムを実行する順序を特定することができ、プログラムの実行順序に従って対応する呼び出しプログラムを実行可能な状態へ復帰させ、第１の記憶手段に書き込む。これにより、一の分割されたプログラムが他の分割されたプログラムを呼び出す場合にのみ対応する呼び出しプログラムが実行可能な状態へ復帰され、第１の記憶手段に書き込まれるので、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、第１の記憶手段に書き込まれている呼び出しプログラムに関係のない分割されたプログラムの実行順序、実行タイミング等を解析することは困難であり、実行するプログラム全体の安全性を確保することが可能となる。

【発明の効果】

【００２２】

第１発明によれば、プログラム実行時にプログラムのすべての内容が第１の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第１の記憶手段へ書き込まれていることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができないことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

【００２３】

また、第２発明によれば、実行要求が出された時点で初めて第１の記憶手段へプログラムが記憶されることから、実行要求が出されるまではプログラムの一部は第１の記憶手段へ書き込まれておらず、外部から第１の記憶手段の内容を参照した場合であってもプログラム全体の内容を把握することは困難であり、実行するプログラムの安全性をより高めることが可能となる。

【００２４】

また、第３発明によれば、重要性、秘匿性等の低いプログラムは第１の記憶手段上に常時書き込んでおき、重要性、秘匿性等の高いプログラムは実行時のみ第１の記憶手段に書き込むことで、必要なプログラムのみ実行の安全性を高めることができ、安全性を確保するための処理によるプログラムのオーバヘッドを低減することが可能となる。

【００２５】

また、第４発明によれば、プログラム実行時にプログラムのすべての内容が第１の記憶手段上に書き込まれていることがなく、実行時には部分的なプログラムのみが第１の記憶手段へ書き込まれていることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム全体の内容を取得することができない

ことからプログラム内容を解析することができず、実行するプログラムの安全性を確保することが可能となる。

【００２６】

また、第５発明によれば、記憶されているプログラムの分割に関する情報に基づいて適正にプログラムを分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが第１の記憶手段に書き込まれる状態が生じることを回避し、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。

【００２７】

また、第６発明によれば、プログラム実行時に分割されたプログラムは第１の記憶手段上に書き込まれているが、分割されたプログラム間の関係が不明であることから、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、分割されたプログラムの実行順序、実行タイミング等を解析することが困難であり、実行するプログラムの安全性を確保することが可能となる。

【００２８】

また、第７発明によれば、一の分割されたプログラムが他の分割されたプログラムを呼び出す場合にのみ対応する呼び出しプログラムが実行可能な状態へ復帰され、第１の記憶手段に書き込まれるので、悪意ある第三者が第１の記憶手段の内容のイメージコピーを不正に取得した場合であっても、第１の記憶手段に書き込まれている呼び出しプログラムに関係のない分割されたプログラムの実行順序、実行タイミング等を解析することは困難であり、実行するプログラム全体の安全性を確保することが可能となる。

【発明を実施するための最良の形態】

【００２９】

以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

【００３０】

（実施の形態１）

以下、本発明の実施の形態１に係る情報処理装置について図面に基づいて具体的に説明する。本実施の形態１では、情報処理装置として一つのコンピュータ、例えばＰＣを用いて具現化する場合について説明する。もちろん、実行されるプログラムで使用されるデータは、通信手段を介して接続された他のＰＣ、又はＤＶＤ等の可搬型記録媒体に記録されていてもよく、通信手段についても特に限定されるものではない。

【００３１】

図１は、本発明の実施の形態１に係る情報処理装置の概略構成図である。図１に示すように、情報処理装置１は、少なくとも、ＣＰＵ（中央演算装置）１１、ＲＯＭ１２、ＲＡＭ（第１の記憶手段）１３、記憶手段（第２の記憶手段）１４、外部の通信手段と接続する通信インタフェース１５、マウス、キーボード等の入力手段と接続する入力インタフェース１６、ＬＣＤ、モニタ、スピーカ等の出力手段と接続する出力インタフェース１７、及びセキュアモジュール２０と接続するセキュアインタフェース１８で構成される。

【００３２】

記憶手段１４は、ハードディスクに代表される固定型記録媒体、又はＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体であり、実行するプログラム、実行するプログラムで使用されるデータ等を記録する第２の記憶手段である。なお、第２の記憶手段としては、記憶手段１４に限定されるものではなく、例えば実行するプログラム、実行するプログラムで使用されるデータ等を記憶するＲＯＭ１２であってもよい。

【００３３】

情報処理装置１は、取り外し可能なセキュアモジュール２０を着脱可能なセキュアインタフェース１８を有する。セキュアインタフェース１８は、例えばＰＣＩバスを介してセキュアモジュール２０を接続する。セキュアモジュール２０は、例えばＰＣカードによって構成され、ＤＭＡ（Direct Memory Access）により、ＣＰＵ１１と独立してＲＡＭ１３

ヘアクセスすることが可能である。セキュアモジュール２０は、ＴＲＭ（Tamper Resistant Module）構造を有しており、外部から第三者による内容の閲覧を防止することができるとともに、内部データの改竄を防止することができるようになっている。

【００３４】

図２は、セキュアモジュール２０の構成の例示図である。図２に示すように、セキュアモジュール２０は、プロセッサ２１、メモリ２２、情報処理装置１のセキュアインタフェース１８を介して通信する通信手段２３を含むＬＳＩを備える。メモリ２２は、外部から参照できない不揮発性のフラッシュメモリ（ＥＥＰＲＯＭ）であり、プログラムの難読化情報、暗号化鍵、復号化鍵等の第三者に対して秘匿する必要がある情報が記録されている。

【００３５】

情報処理装置１は、セキュアモジュール２０を用いて、プログラムをＲＡＭ１３に書き込んで実行する。記憶手段１４は、セキュアモジュール２０のメモリ２２に記憶している暗号化情報、例えば暗号化鍵によって暗号化されたプログラムを記憶している。また、セキュアモジュール２０へ暗号化されたプログラムを転送することで、メモリ２２に記憶している暗号化鍵を用いて該プログラムを復号化することができる。なお、暗号化鍵単独で暗号化／復号化を行うものに限定されるものではなく、暗号化鍵と復号化鍵とを独立して記憶しているものであってもよい。

【００３６】

記憶手段１４に記憶されているプログラムを実行する場合、まず記憶手段１４に記憶されている暗号化されたプログラムをセキュアモジュール２０へ転送する。セキュアモジュール２０は、転送されたプログラムをメモリ２２に記憶している暗号化鍵を使用して復号するとともに、プログラムの命令コードを解析して、複数のプログラム部品へ分割する。図３は、プログラム分割の例示図である。図３に示すように、分割されたプログラム部品は、プログラム４０の一部を構成するプログラムコードである。プログラム４０が動作するときには、例えばプログラム部品４１～４３が互いに他のプログラム部品４１～４３を呼び出す、又は他のプログラム部品４１～４３へジャンプしながら、１つのプログラム４０として動作する。プログラム部品は、最小単位としてプロセッサの命令１つから構成される。

【００３７】

なお、プログラムの分割については、本実施の形態１のように、セキュアモジュール２０がプログラムを解析してプログラム部品に分割してもよいが、斯かる方法に限定されるものではなく、事前に、プログラム分割に関する情報、例えば分割単位に関する情報を付加して該プログラムを記憶手段１４に記憶しておき、セキュアモジュール２０での復号時に、斯かる情報に基づいて分割する方法であってもよい。プログラム分割に関する情報に基づいてプログラムを分割することで、プログラムを適切に分割することができ、例えば分割単位が不適切であることにより、多くの分割されたプログラムが実行可能な状態でＲＡＭ１３に書き込まれている状態が生じることを回避し、悪意ある第三者がＲＡＭ１３の内容のイメージコピーを不正に取得した場合であっても、プログラム内容の解析をより困難にすることができ、実行するプログラムの安全性を確保することが可能となる。

【００３８】

また、記憶手段１４に暗号化されたプログラムとして記憶する時点で、複数のプログラム部品として記憶するものであってもよい。この場合、セキュアモジュール２０は、転送されたプログラム部品を、メモリ２２に記憶している暗号化鍵を使用して復号する。

【００３９】

次に、セキュアモジュール２０は、最初に動作する部分であるプログラム部品、例えばプログラム部品４１をＲＡＭ１３へ書き込む。ＲＡＭ１３へ書き込まれた後、ＣＰＵ１１は、書き込まれたプログラム部品４１を実行する。プログラム部品４１を実行し、他のプログラム部品の実行を要求する命令コードが存在する場合、該命令コードを実行するタイミングで、セキュアモジュール２０は要求される他のプログラム部品、例えばプログラム

部品４２、４３をＲＡＭ１３へ書き込む。ＣＰＵ１１は、ＲＡＭ１３への書き込み完了通知を受け取った後、書き込まれたプログラム部品４２、４３を順次実行する。

【００４０】

書き込まれたプログラム部品の実行が完了した場合、ＲＡＭ１３へ書き込まれたプログラム部品は、ＣＰＵ１１がＲＡＭ１３から消去する。したがって、プログラム全体がＲＡＭ１３へ書き込まれていることがなく、プログラムを構成するプログラム部品の一部のみがＲＡＭ１３へ書き込まれながら、プログラムが実行される。

【００４１】

このように、プログラム全体をＲＡＭ１３へ書き込まないことから、悪意ある第三者によりＲＡＭ１３のイメージコピーを不正に取得された場合であっても、イメージコピーには、プログラム全体のうちの一部のプログラム部品しか書き込まれておらず、逆解析によりプログラムの全容を把握することが困難であり、実行するプログラムの安全性を確保することが可能となる。

【００４２】

ここで、セキュアモジュール２０は、ＣＰＵ１１と独立して動作する。したがって、ＲＡＭ１３へ書き込まれたプログラムが、他のプログラム部品を必要とするタイミングをセキュアモジュール２０へ通知する必要がある。ＣＰＵ１１が、セキュアモジュール２０へ他のプログラム部品を必要とするタイミングを通知する手段としては種々の方法が用いられる。例えば、実行するプログラムが、セキュアモジュール２０との間で実行タイミングの同期を取ることが可能な構造を有するプログラムである場合、該プログラムが要求するプログラム部品が実行される直前に、セキュアモジュール２０により対応するプログラム部品をＲＡＭ１３へ書き込む方法を用いる。

【００４３】

図４は、実行するプログラムが要求するプログラム部品が実行される直前に、セキュアモジュール２０により対応するプログラム部品をＲＡＭ１３へ書き込む方法の説明図である。図４（ａ）に示すように、プログラムの中に条件分岐命令を設定する。該条件分岐命令の条件は一定値とし、必ず一方の経路を選択するようにしておく。他方の経路には無効なプログラム部品を配置する。無効なプログラム部品は、例えばｎｏｐ列、０列等、動作しないプログラムコードである。なお、無効なプログラム部品が配置された領域に、要求されたプログラム部品の書き込み可能領域を確保しておく。

【００４４】

セキュアモジュール２０は、ＲＡＭ１３へ書き込まれていないプログラム部品の実行が必要になったタイミング、すなわちプログラム部品の実行要求命令がプログラムで実行された時点で、図４（ｂ）に示すように、ＲＡＭ１３の無効なプログラム部品が配置された領域のプログラム部品の書き込み可能領域に、要求されたプログラム部品を書き込む。なお、ＲＡＭ１３へ該プログラム部品が書き込まれた後、図４（ｃ）に示すように該プログラム部品を要求したプログラムの条件分岐命令の条件を変更し、他方の経路を選択するようにして、ＣＰＵ１１が、書き込まれたプログラム部品を実行する。

【００４５】

実行されるプログラムが、セキュアモジュール２０との間で実行タイミングの同期を取ることが可能な構造を有さないプログラムである場合、セキュアモジュール２０は、プログラムをＲＡＭ１３へ書き込む時点で、プログラム部品の実行を要求する実行要求プログラムを該プログラムへ挿入する。セキュアモジュール２０は、挿入した実行要求プログラムの実行に応じて、対応するプログラム部品をＲＡＭ１３へ書き込む。

【００４６】

プログラムのうち、どのプログラム部品を常にＲＡＭ１３へ書き込み、どのプログラム部品をいつＲＡＭ１３へ書き込むべきかについては、事前にセキュアモジュール２０に書込情報として記憶しておく。これにより、重要な秘密情報を扱うプログラム部品がＲＡＭ１３に常駐することを回避することができ、より安全性を高めることができる。書込情報としては、「常にＲＡＭ１３へ書き込み」、「実行時にＲＡＭ１３へ書き込み」、「セキ

ュアモジュールが選択」の３種類がある。

【００４７】

図５は、プログラム部品を動的にＲＡＭ１３へ書き込む場合の説明図である。図５（ａ）に示すように、プログラムの実行開始時には、プログラム部品４１をＲＡＭ１３へ書き込む。プログラム部品４２はＲＡＭ１３へ書き込まず、セキュアモジュール２０に対してプログラム部品４２の実行要求を行う実行要求プログラム５０をＲＡＭ１３へ書き込む。実行要求プログラム５０は、セキュアモジュール２０で生成してもよいし、あらかじめセキュアモジュール２０に記録しておいてもよい。プログラム部品４１は、プログラム部品４２を呼び出すプログラムではなく、実行要求プログラム５０を呼び出す。

【００４８】

プログラムが実行されると、プログラム部品４１は、最後に実行要求プログラム５０を呼び出す。実行要求プログラム５０が実行されると、図５（ｂ）に示すように、セキュアモジュール２０は、要求されたプログラム部品４２をＲＡＭ１３へ書き込む。セキュアモジュール２０によりプログラム部品４２がＲＡＭ１３へ書き込まれた後、ＣＰＵ１１がプログラム部品４２を実行することにより、プログラム部品４２をプログラム部品４１から直接呼び出した場合と同様に実行することができる。

【００４９】

セキュアモジュール２０は、プログラム部品４２のＲＡＭ１３への書き込みの完了を検知するため、実行要求プログラム５０の末尾に、例外処理を生じる命令を設定しておく。ＣＰＵ１１が、実行要求プログラム５０を実行し、末尾に設定された例外処理を生じる命令を実行した場合、ＣＰＵ１１は、プログラムの実行を一旦停止させ、セキュアモジュール２０に対してＲＡＭ１３への書き込み完了通知を送信する。これにより、セキュアモジュール２０は、割り込み命令、アクセス違反等の例外処理を生じる命令を実行要求プログラム５０に付加し、実行要求プログラム５０を実行するだけであることから、例えばプログラムの待機を行うプログラムを直接呼び出す場合のように、待機処理を行っているプログラムを特定することが困難になる。したがって、第三者にとってはより解析しにくい形でプログラム部品のＲＡＭ１３への書き込みの完了を待つことが可能となる。

【００５０】

以上のように本実施の形態１によれば、セキュアモジュール２０がプログラムを複数のプログラム部品に分割し、分割されたプログラム部品単位でＲＡＭ１３へ書き込み、実行することから、悪意ある第三者にＲＡＭ１３のイメージコピーを取得された場合であっても、プログラムの全体像を把握することが困難であり、プログラムの安全性を確保することが可能となる。

【００５１】

（実施の形態２）

実施の形態２に係る情報処理装置１は、実施の形態１と同様の構成であるが、実施の形態１のようにプログラム部品自体をセキュアモジュール２０から動的にＲＡＭ１３へ書き込むのではなく、プログラム部品はＲＡＭ１３へ常時書き込んでおき、各プログラム部品中の他のプログラム部品の呼び出しアドレスだけを更新する。図６は、本実施の形態２に係る情報処理装置でのプログラム部品実行方法の説明図である。

【００５２】

図６（ａ）に示すように、最初のプログラムをＲＡＭ１３へ書き込んだ時点では、プログラム部品４１からプログラム部品４２、４３を呼び出す部分には無効なアドレスを記録しておく。したがって、イメージコピーを取得した第三者が解析しても、プログラム部品４１がどのプログラム部品をプログラム実行中に呼び出すのか不明となる。そして、図６（ｂ）に示すように、プログラム部品４１からプログラム部品４２、４３を呼び出すタイミングで、セキュアモジュール２０は、プログラム部品４１の中の呼び出しアドレスを、次に実行するプログラム部品が存在するアドレスへ書き換える。この結果、プログラム部品４１からプログラム部品４２が呼び出され、プログラム部品４２を実行することができる。

【００５３】
以上のように本実施の形態２によれば、実施の形態１のようにプログラム部品自体をＲＡＭ１３へ書き込むのではなく、呼び出しアドレスの書き換えのみを行えばよいことから、プログラム部品をＲＡＭ１３へ書き込む時間に比べて短時間でアドレス書き換えを行うことができ、全体の処理時間を短縮することが可能となる。
【００５４】
なお、実施の形態１及び２を組み合わせることにより、呼び出し元プログラム部品の呼び出し先アドレスの書き換えと、プログラム部品のＲＡＭ１３への書き込みを同時に行い、プログラム部品が動的にＲＡＭ１３へ書き込まれ、かつＲＡＭ１３へ書き込まれるごとに呼び出しアドレスが変化するようにしてもよい。これにより、より実行するプログラムの安全性を高めることが可能となる。
【００５５】
（実施の形態３）
以下、実行するプログラムを事前に分割してＲＡＭ１３へ書き込む場合の実施例について説明する。図７は、本発明の実施の形態３に係る情報処理装置１で実行するプログラムのプログラム部品への分割の説明図である。図７に示すように、実行するプログラム４０を、あらかじめプログラム部品４１～４３に分割しておき、分割されたプログラム部品４１～４３に対して、それぞれ書込情報４１０～４３０、特殊コード情報４１１～４３１、部品リンク情報４１２～４３２からなる付加情報を記憶する。書込情報４１０～４３０は、プログラム部品４１～４３をＲＡＭ１３へどのタイミングで書き込むのかを示す情報である。特殊コード情報４１１～４３１は、プログラム部品４１～４３が特殊コードであるか否か、及びどのような特殊コードであるのかを示す情報である。部品リンク情報４１２～４３２は、プログラム部品同士がどのように呼び出されるかを記述する情報である。
【００５６】
図８は、書込情報４１０、特殊コード情報４１１、及び部品リンク情報４１２の例示図である。プログラム部品４１は、ＣＰＵ１１が実行可能なプログラムコードである。書込情報４１０は、「常にメモリに書き込む」という情報を記憶している。特殊コード情報４１１は、「オフセット50hのアドレスから秘密データを渡す特殊コードである」という情報を記憶している。部品リンク情報４１２は、「オフセット100hのアドレスからプログラム部品４２のオフセットアドレス10hを呼び出す」、及び「アドレス320hからプログラム部品４３のオフセットアドレス30hを呼び出す」という情報を記憶している。
【００５７】
なお、部品リンク情報は複数の情報を含んでもよい。また、特殊コード情報も複数の特殊コード情報を含んでもよい。これらプログラム部品に関する情報は、セキュアモジュール２０の外部から参照することができないメモリ２２に記憶されている暗号化鍵で暗号化され、セキュア化プログラムデータ３０として記憶手段１４に記憶される。
【００５８】
図９は、プログラムの実行開始時の動作の説明図である。プログラムを実行する場合、まず基本プログラム６０が動作する。基本プログラム６０は、記憶手段１４からセキュア化プログラムデータ３０を読み出す。次に、基本プログラム６０は、プログラム４０が動作するための実行領域１００をＲＡＭ１３に確保する。そしてセキュア化プログラムデータ３０と、プログラム実行用に確保した実行領域１００のアドレスをセキュアモジュール２０に渡す。
【００５９】
セキュアモジュール２０は、セキュア化プログラムデータ３０を外部から参照することができないメモリ２２に記憶されている暗号化鍵を用いて復号する。そして、実行すべきプログラム部品４１をＲＡＭ１３の実行領域１００へ書き込む。ＣＰＵ１１は、基本プログラム６０にて実行領域１００へ書き込まれたプログラム部品４１の開始アドレスが呼び出された場合、プログラム部品４１の実行を開始する。
【００６０】

図１０は、プログラムの実行開始時のセキュアモジュール２０での処理のフローチャートである。図１０に示すように、セキュアモジュール２０は、セキュア化プログラムデータ３０を外部から参照することができないメモリ２２に記憶されている暗号鍵を用いて復号する（ステップＳ１００１）。セキュア化プログラムデータ３０を復号した後、各プログラム部品に付加されている書込情報の内容を確認する（ステップＳ１００２）。書込情報にＲＡＭ１３へ書き込む旨が記憶されている場合（ステップＳ１００３：ＹＥＳ）、記憶されているプログラム部品をＲＡＭ１３の実行領域１００へ書き込む（ステップＳ１００４）。

【００６１】

次に、セキュアモジュール２０は、プログラム部品の特殊コード情報の有無を確認する（ステップＳ１００５）。特殊コード情報が有る場合（ステップＳ１００６：ＹＥＳ）、特殊コードに従った呼び出し処理を実行する（ステップＳ１００７）。特殊コード呼び出し処理の詳細については後述する。すべてのプログラム部品について上述した処理を繰り返す（ステップＳ１００８）。

【００６２】

すべてのプログラム部品につき上述した処理が完了した場合（ステップＳ１００８：ＹＥＳ）、プログラム部品間のリンク処理を実行する（ステップＳ１００９）。プログラム部品間のリンク処理の詳細についても後述する。リンク処理が完了した時点でプログラムの実行準備が完了する。プログラムの実行準備が完了した旨は、割り込み処理、状態レジスタ等により情報処理装置（ＰＣ）１に通知する。

【００６３】

セキュアモジュール２０が行う特殊コード呼び出し処理は、セキュアモジュール２０が動作タイミングを制御する部分のプログラムコード呼び出し処理である。図１１及び図１２は、セキュアモジュール２０が行う特殊コード呼び出し処理の説明図である。図１１は、特殊コード情報、リンク情報等の例示図である。図１１の例では、プログラム部品４１には、「オフセット50hのアドレスからプログラム部品４５を呼び出す」という部品リンク情報４１２が付加されている。また、プログラム部品４５は、「コンテンツ鍵変更時に実行」という特殊コード情報４５１を含んでいる。

【００６４】

セキュアモジュール２０は、特殊コード呼び出し部８０をＲＡＭ１３へ書き込み、特殊コード呼び出し部８０をプログラム部品４１から呼び出すようリンクする。特殊コード呼び出し部８０は、セキュアモジュール２０で自動生成してもよいし、プログラム部品としてセキュア化プログラムデータ３０に含めておいてもよい。

【００６５】

ＲＡＭ１３へ書き込んだ特殊コード呼び出し部８０は、条件分岐から参照されるデータ、条件分岐コード及び特殊コードを呼び出す部分からなる。図１２（ａ）には、特殊コード呼び出し部８０がアドレス13845fa0hに書き込まれる例が示されている。その先頭には条件分岐で参照されるデータが埋め込まれている。

【００６６】

通常、先頭に埋め込まれる条件分岐で参照される値は０である。特殊コードの実行条件を具備しない間は０のままである。図１２（ａ）の条件分岐では、アドレス13845fa0hに記憶された値が０である場合、即座にリターンするようにしておく。これにより、プログラム部品４１から特殊コード呼び出し部８０が呼び出された場合であっても、特殊コードの実行条件を具備しない場合は即座にリターンすることができる。

【００６７】

条件分岐で参照される値が０でない場合は、続くプログラムコードが実行される。続くプログラムコードは、分岐条件で参照される値に０を設定するコードと、プログラムの実行領域１００を呼び出すコードから構成される。プログラム実行開始時の初期書き込み時には、プログラムの実行領域１００には無効なプログラムデータが書き込まれている。

【００６８】

プログラムの実行中に、特殊コードの実行条件を具備した場合、セキュアモジュール２０は、実行領域１００に、実行条件を具備した特殊コードを書き込む。図１２（ｂ）の例では、特殊コードは「コンテンツ鍵変更時に実行」されるというコードであることから、セキュアモジュール２０は、コンテンツ鍵の変更直前に実行領域１００へプログラム部品４５を書き込む。プログラム部品４５を書き込んだ後、アドレス13845fa0hの条件分岐から参照されるデータを書き換える。書き換えることにより、特殊コードの実行条件を具備した状態となる。特殊コードの実行条件を具備した状態で、特殊コード呼び出し部８０が実行されると、即座にリターンすることなく、条件分岐で参照される値に０を設定するコードと、プログラム部品４５を呼び出すコードが実行される。

【００６９】

次にセキュアモジュール２０が実行するプログラムリンク処理について述べる。プログラムリンク処理は、任意のプログラム部品を動的に書き込む処理である。図１３及び図１４は、プログラム部品の動的書き込み処理及びリンク処理についての説明図である。図１３は、プログラム部品４１に関連する書き込み処理及びリンク処理での書込情報、リンク情報等の例示図である。

【００７０】

図１３の例では、プログラム部品４１に対応する部品リンク情報４１２から、プログラム部品４１はプログラム部品４２とプログラム部品４３の呼び出しを含んでいることがわかる。それぞれの書込情報４２０、４３０を参照すると、プログラム部品４２は実行時までＲＡＭ１３に書き込まず、プログラム部品４３は開始時にＲＡＭ１３に書き込まれるように記述されている。プログラム部品４３は常にＲＡＭ１３に書き込まれるコードであることから、プログラム部品４１の実行開始時に、プログラム部品４１からプログラム部品４３の呼び出しは実行される。

【００７１】

図１４（ａ）では、プログラム部品４３は、ＲＡＭ１３のアドレス13900000hの領域に書き込まれている。そこで、プログラム部品４１のオフセット320ｈにあるプログラム部品４３の呼び出しコマンドには、プログラム部品４３のアドレスを設定する。本実施例では、プログラム部品４３のオフセット30hを呼び出しているので、プログラム部品４１には、13900030hを呼び出すよう呼び出しコマンドの呼び出し先アドレスを設定しておく。

【００７２】

一方、プログラム部品４２は、プログラム部品４１の実行開始時にＲＡＭ１３に書き込まれていないので、プログラム部品４２の実行依頼コードをＲＡＭ１３へ書き込んでおき、プログラム部品４１からは実行依頼コードを呼び出すようにしておく。実行依頼コードは、例えばセキュアモジュール２０のレジスタアドレスへの書き込みプログラムにより実現される。

【００７３】

実行依頼コードの末尾には、例外処理を発生するコードと、キャッシュフラッシュ命令と、プログラム部品４２本体の呼び出しコードとが含まれる。本実施例では例外処理を発生するコードとしてint 3命令を使用しているが、これ以外の例外処理、例えばメモリアクセス違反を起こすようなコードを使用してもよい。また、プログラム部品４２の書き込まれるアドレスが一定ではないようにしており、呼び出しアドレスには無効な値を記憶している。さらに、キャッシュフラッシュ命令を用いてキャッシュを一旦クリアし、セキュアモジュール２０が設定した呼び出しアドレスが確実に呼び出されるようにしている。キャッシュフラッシュ命令はアーキテクチャに依存するものであることから、アーキテクチャによっては使用できない。

【００７４】

プログラムの実行が開始される場合、図１４(ｂ)に示すように、プログラム部品４１が実行され、プログラム部品４２の実行依頼コードが実行されると、ＰＣからセキュアモジュール２０に、プログラム部品４２のＲＡＭ１３への書き込みが要求される。そして、プログラムは、次の例外処理発生コード(int 3)を実行し、割り込みハンドラが起動される

。割り込みハンドラは、セキュアモジュール２０からのプログラム書き込み完了割り込み処理が発生するまで待機し、割り込み処理の発生後、続きのコードを実行するようにしておく。実行依頼を受けたセキュアモジュール２０は、プログラム部品４２をＲＡＭ１３へ書き込むと共に、呼び出し元の呼び出し先アドレスを設定する。

【００７５】

本実施例では、アドレス13A00000hの領域にプログラム部品４２を書き込むと共に、呼び出し先アドレスを13A00010h（プログラム部品４２のオフセット10h）に設定している。プログラム部品４２の書き込みは、事前に書き込んでおいてもよいし、プログラム部品４２の呼び出しアドレスを固定しておいてもよい。

【００７６】

以上説明したように、本発明ではセキュアモジュールを利用し、プログラムを動的にＲＡＭ上に書き込み又はプログラムの呼び出しアドレスを動的に変更することにより、悪意ある第三者にとって解析が困難な形態でプログラムを実行することが可能となる。

【図面の簡単な説明】

【００７７】

【図１】本発明の実施の形態１に係る情報処理装置の概略構成図である。

【図２】セキュアモジュールの構成の例示図である。

【図３】プログラム分割の例示図である。

【図４】プログラム部品をＲＡＭへ記憶する方法の説明図である。

【図５】プログラム部品を動的にＲＡＭへ記憶する場合の説明図である。

【図６】本実施の形態２に係る情報処理装置でのプログラム部品実行方法の説明図である。

【図７】本発明の実施の形態３に係る情報処理装置で実行するプログラムのプログラム部品への分割の説明図である。

【図８】書込情報、特殊コード情報、及び部品リンク情報の例示図である。

【図９】プログラムの実行開始時の動作の説明図である。

【図１０】プログラムの実行開始時のセキュアモジュールでの処理のフローチャートである。

【図１１】セキュアモジュールが行う特殊コード呼び出し処理の説明図である。

【図１２】セキュアモジュールが行う特殊コード呼び出し処理の説明図である。

【図１３】プログラム部品の動的書き込み処理及びリンク処理についての説明図である。

【図１４】プログラム部品の動的書き込み処理及びリンク処理についての説明図である。

【符号の説明】

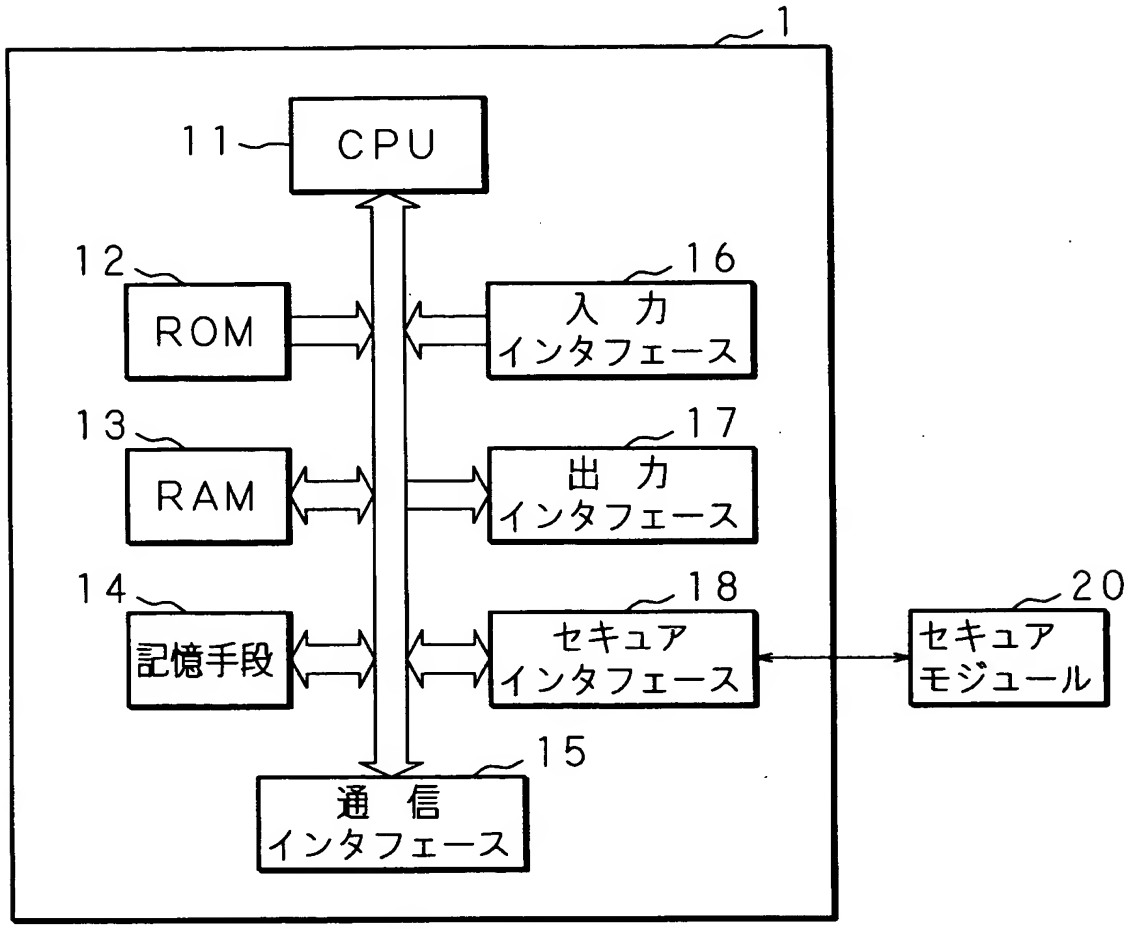
【００７８】

１１　ＣＰＵ
１２　ＲＯＭ
１３　ＲＡＭ（第１の記憶手段）
１４　記憶手段（第２の記憶手段）
１５　通信インタフェース
１６　入力インタフェース
１７　出力インタフェース
１８　セキュアインタフェース
２０　セキュアモジュール
２１　プロセッサ
２２　メモリ
２３　通信手段
３０　プログラムデータ
４０　プログラム

４１、４２、４３、４５　プログラム部品
５０　実行要求プログラム
６０　基本プログラム
８０　特殊コード呼び出し部
１００　実行領域
４１０、４２０、４３０　書込情報
４１１、４２１、４３１、４５１　特殊コード情報
４１２、４２２、４３２　部品リンク情報

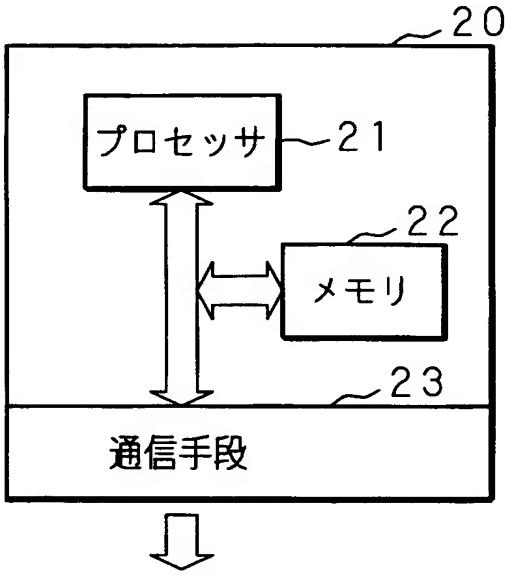
【書類名】図面
【図１】

本発明の実施の形態１に係る情報処理装置の概略構成図



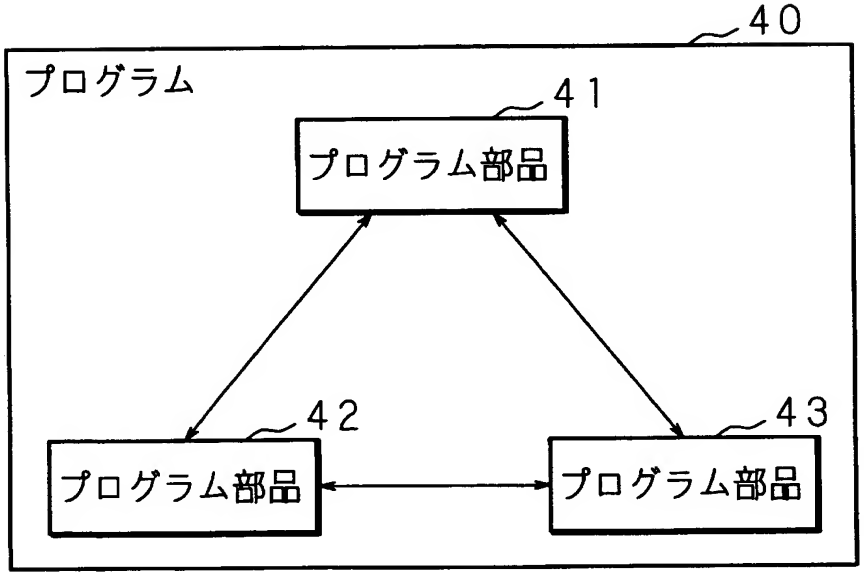
【図２】

セキュアモジュールの構成の例示図



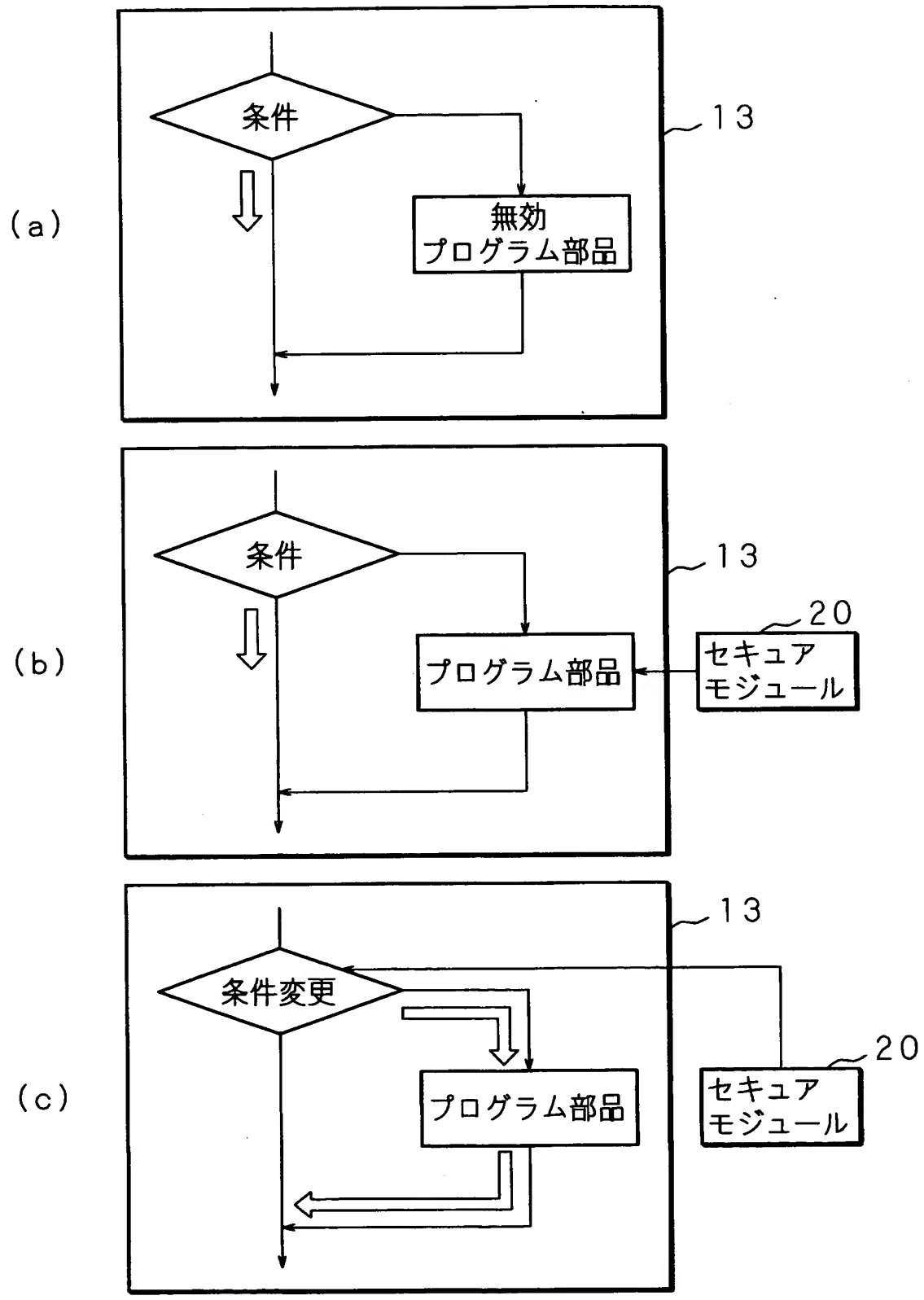
【図３】

プログラム分割の例示図



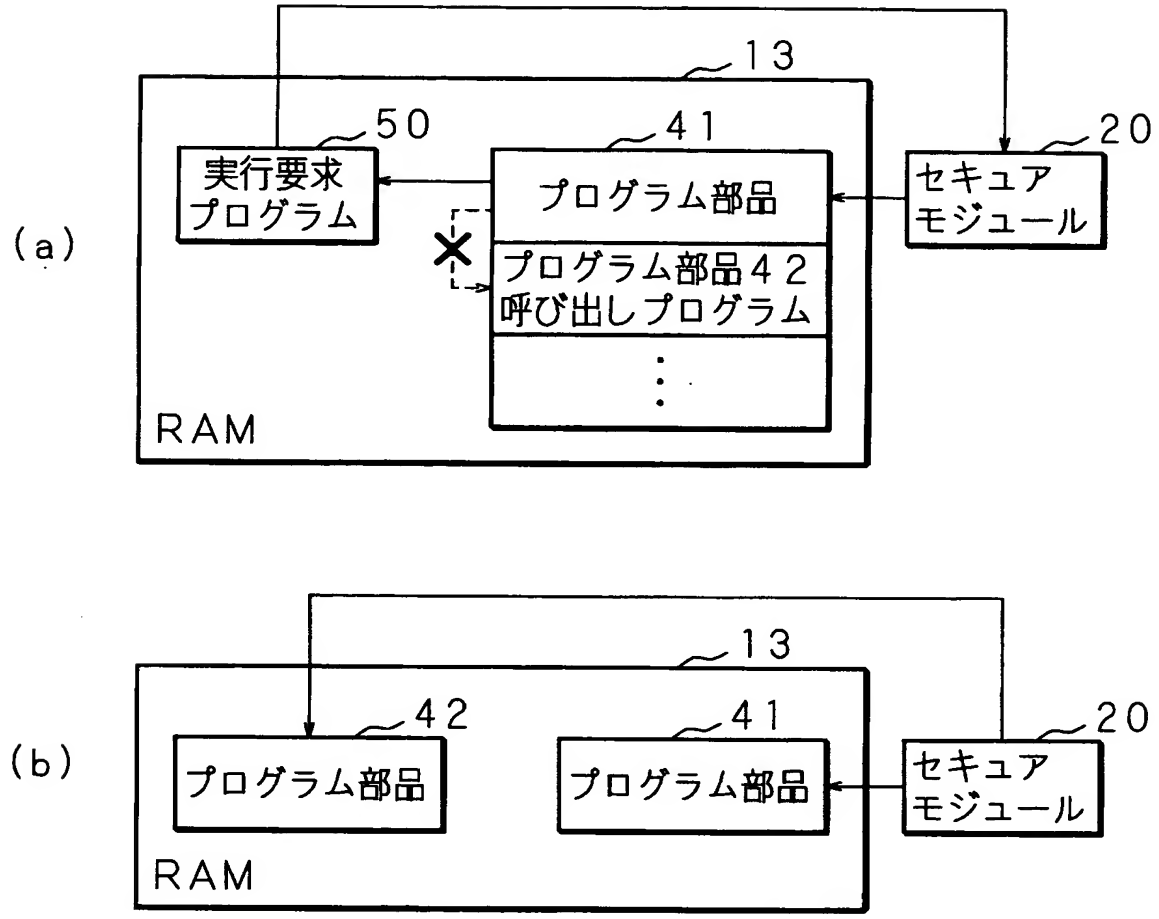
【図４】

プログラム部品をＲＡＭへ記憶する方法の説明図



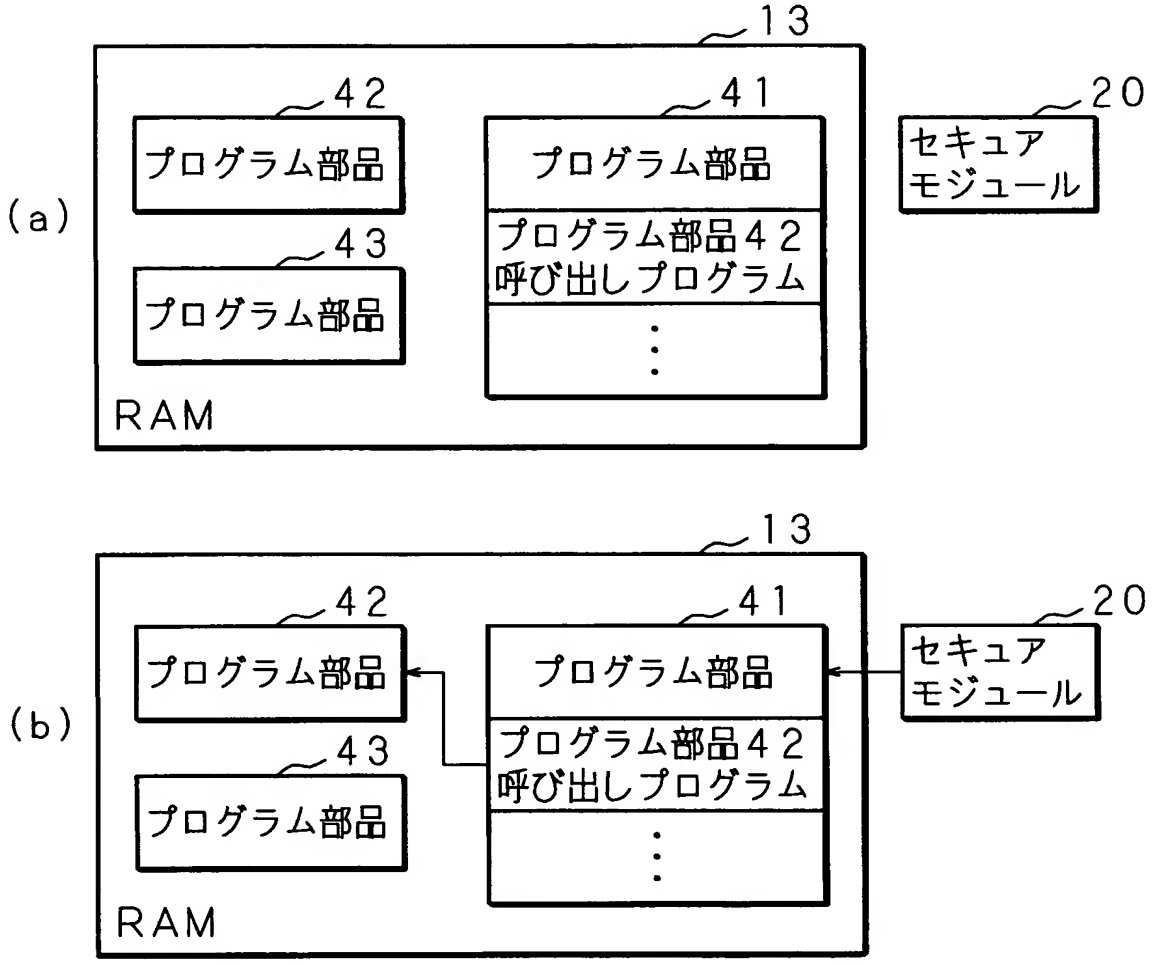
【図５】

プログラム部品を動的にＲＡＭへ記憶する場合の説明図



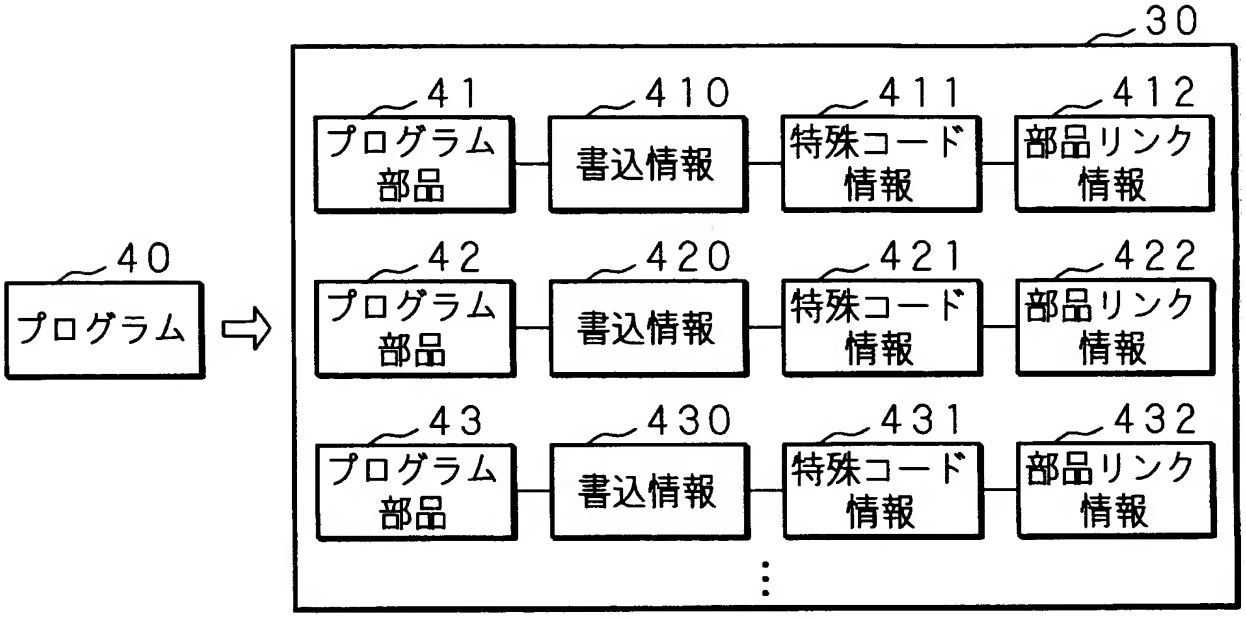
【図６】

本実施の形態２に係る情報処理装置での
プログラム部品実行方法の説明図



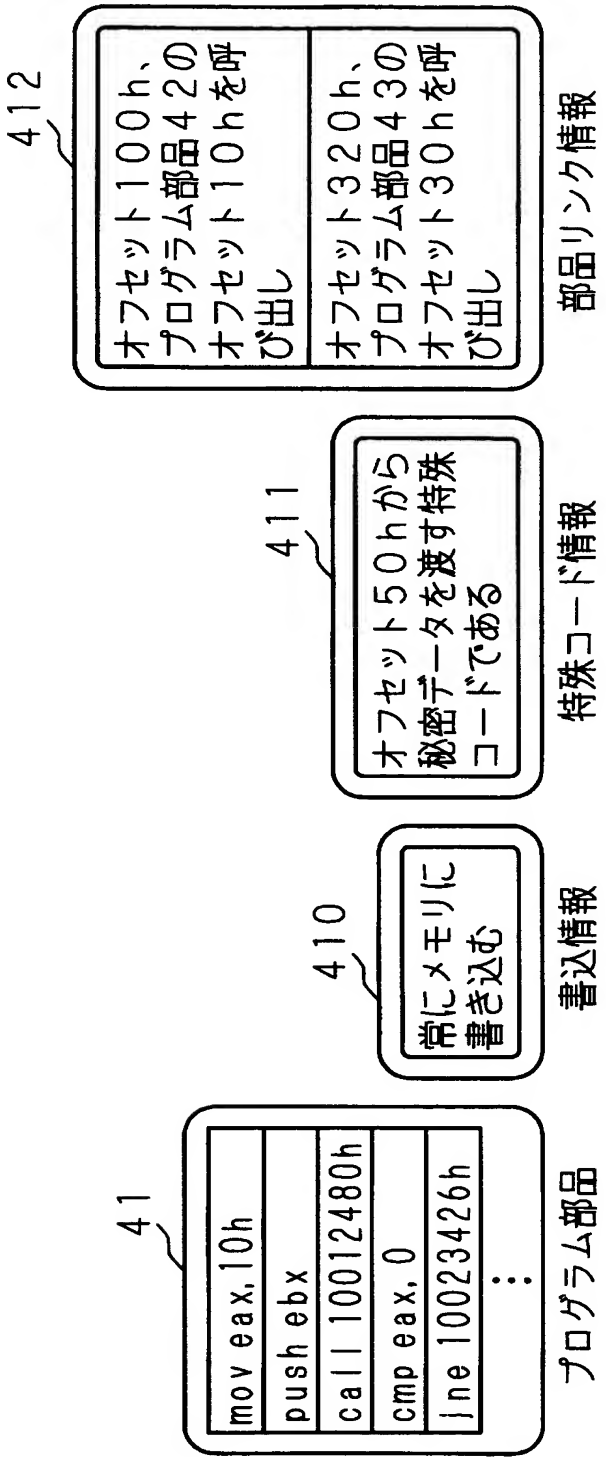
【図７】

本発明の実施の形態３に係る情報処理装置で実行する
プログラムのプログラム部品への分割の説明図



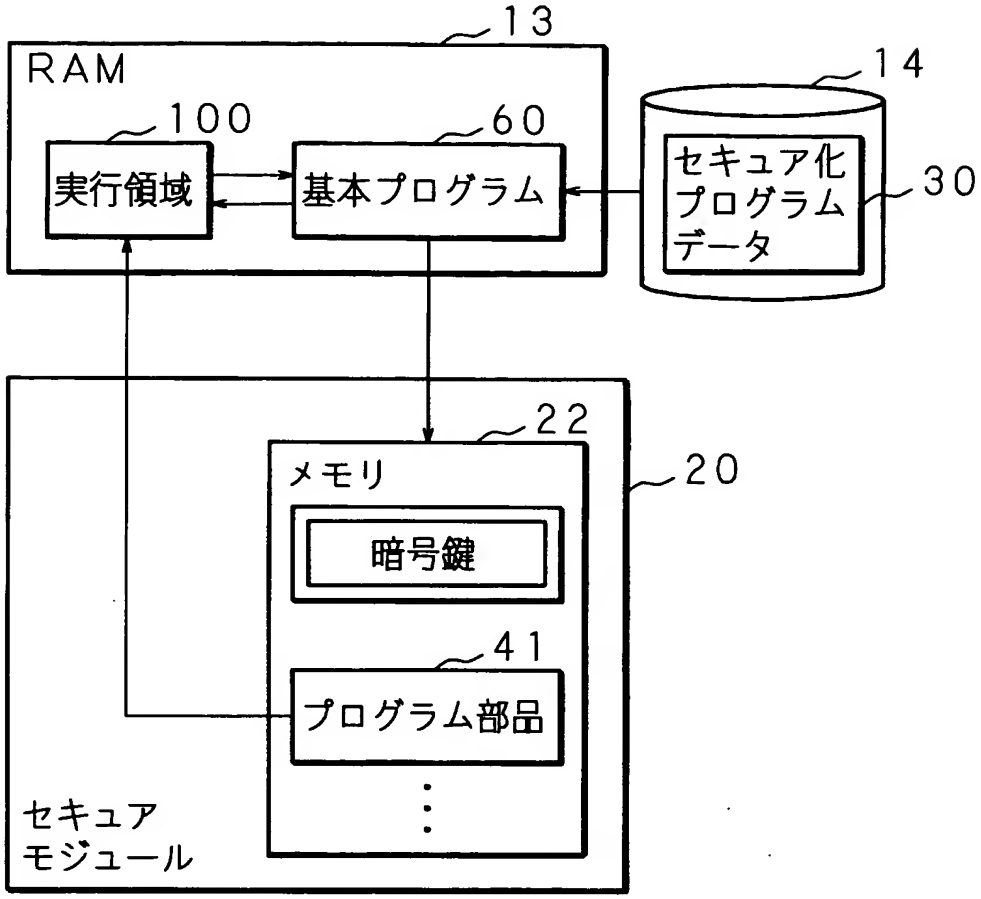
【図８】

書込情報、特殊コード情報、及び部品リンク情報の例示図



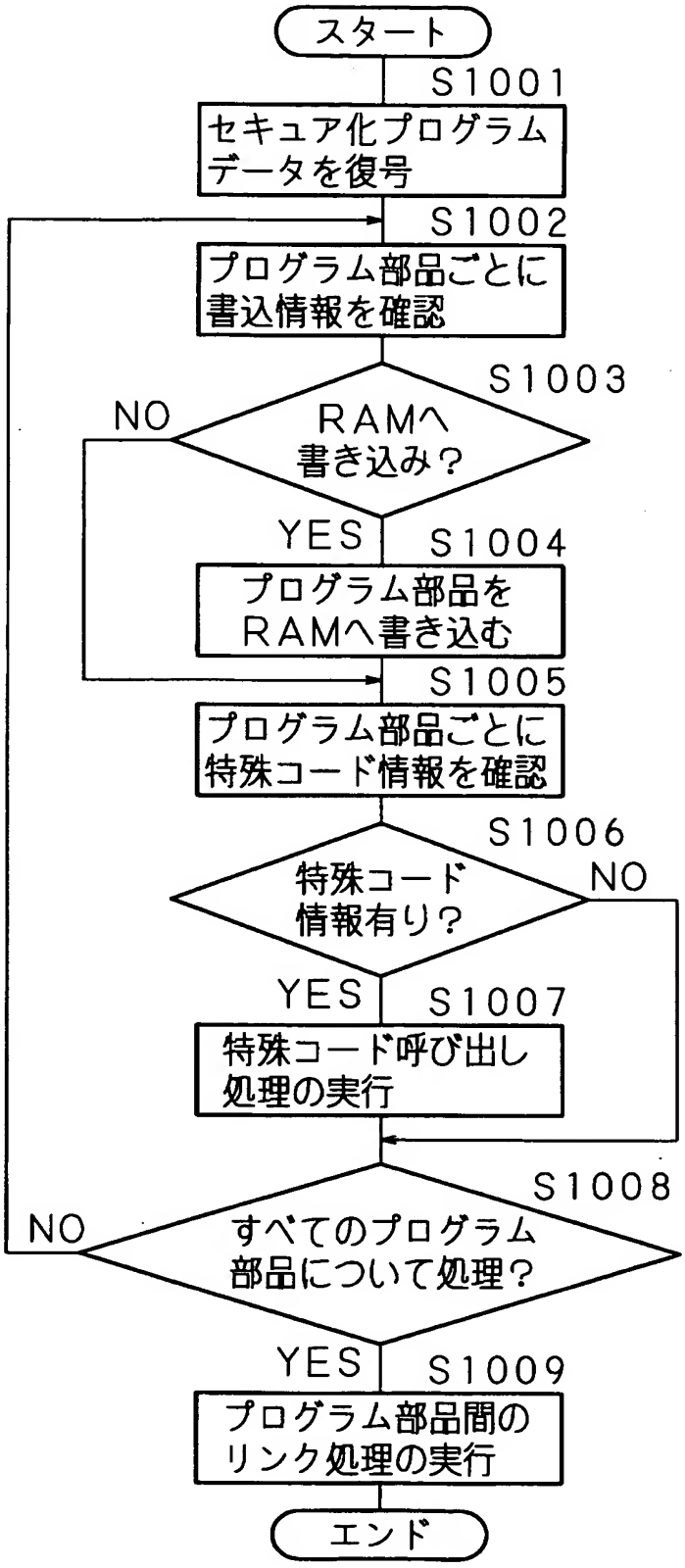
【図９】

プログラムの実行開始時の動作の説明図



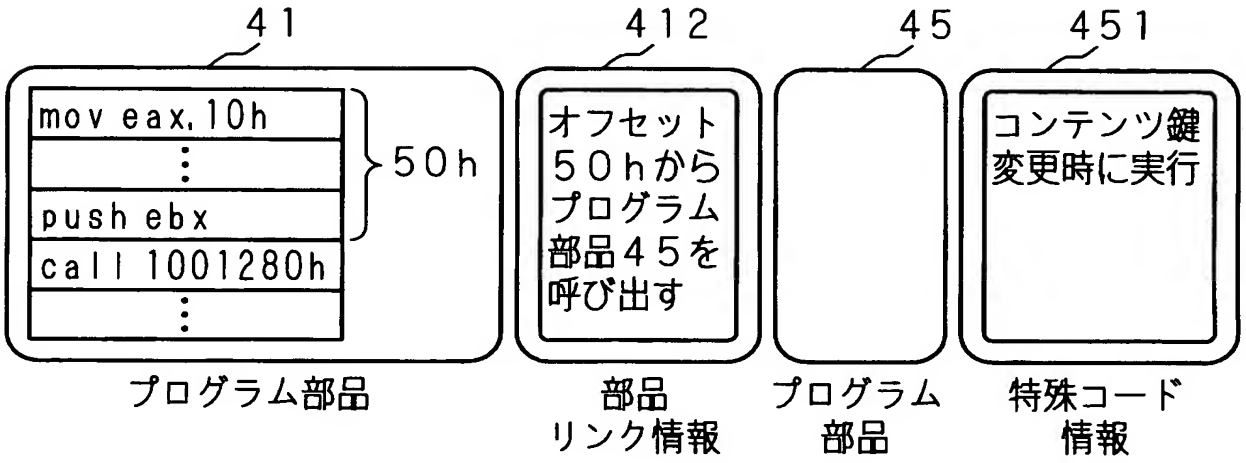
【図１０】

プログラムの実行開始時のセキュアモジュールでの処理のフローチャート



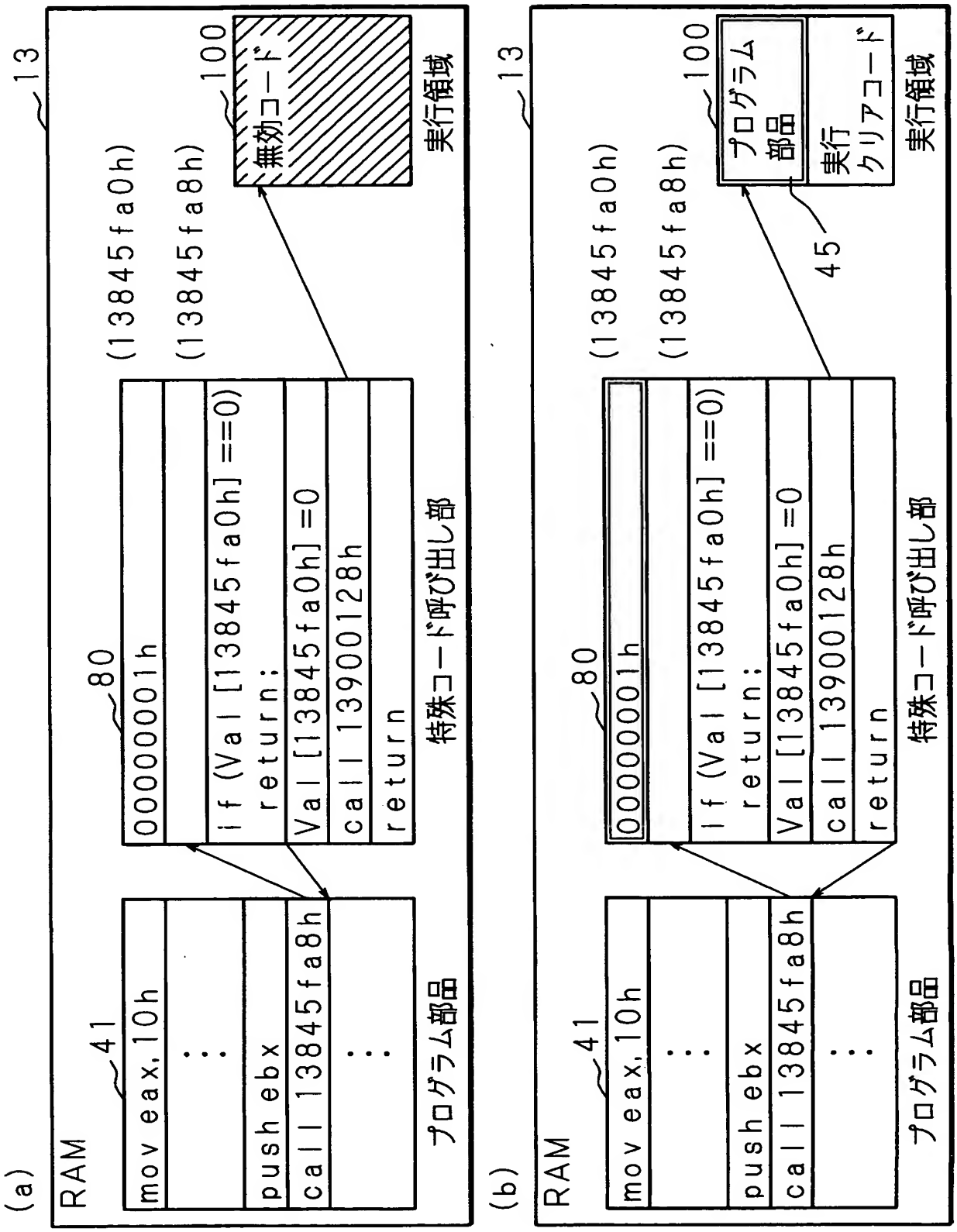
【図１１】

セキュアモジュールが行う特殊コード呼び出し処理の説明図



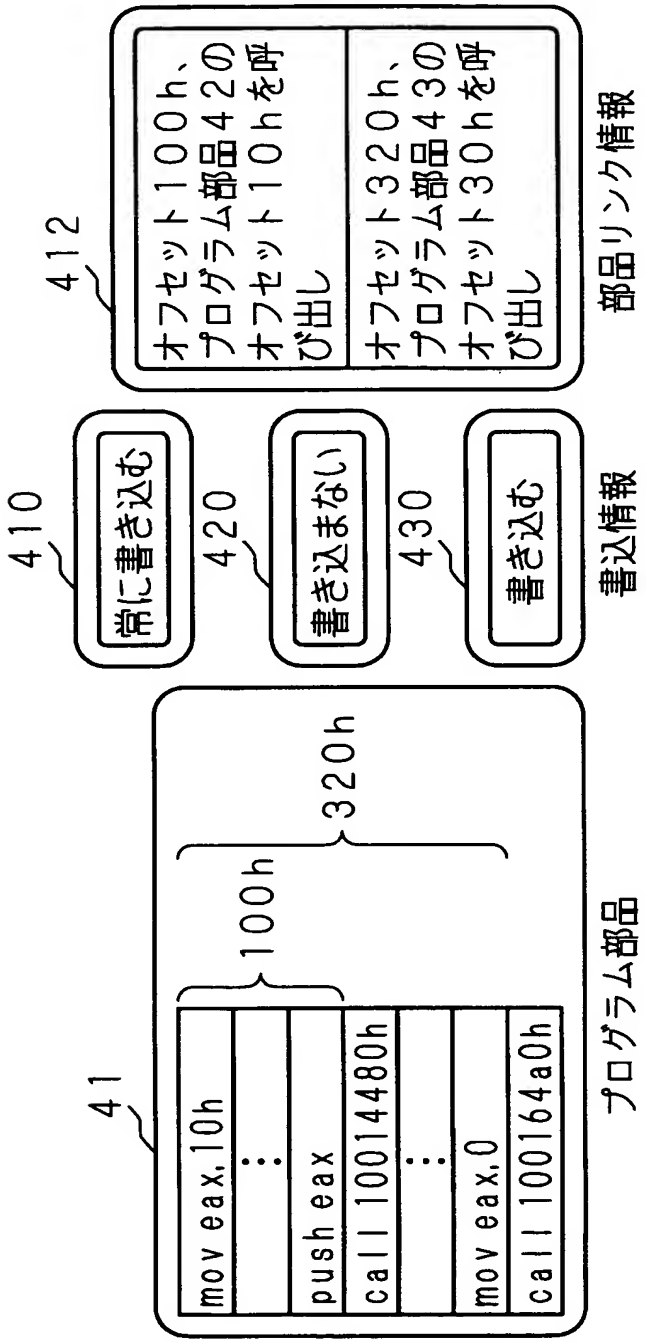
【図１２】

セキュアモジュールが行う特殊コード呼び出し処理の説明図



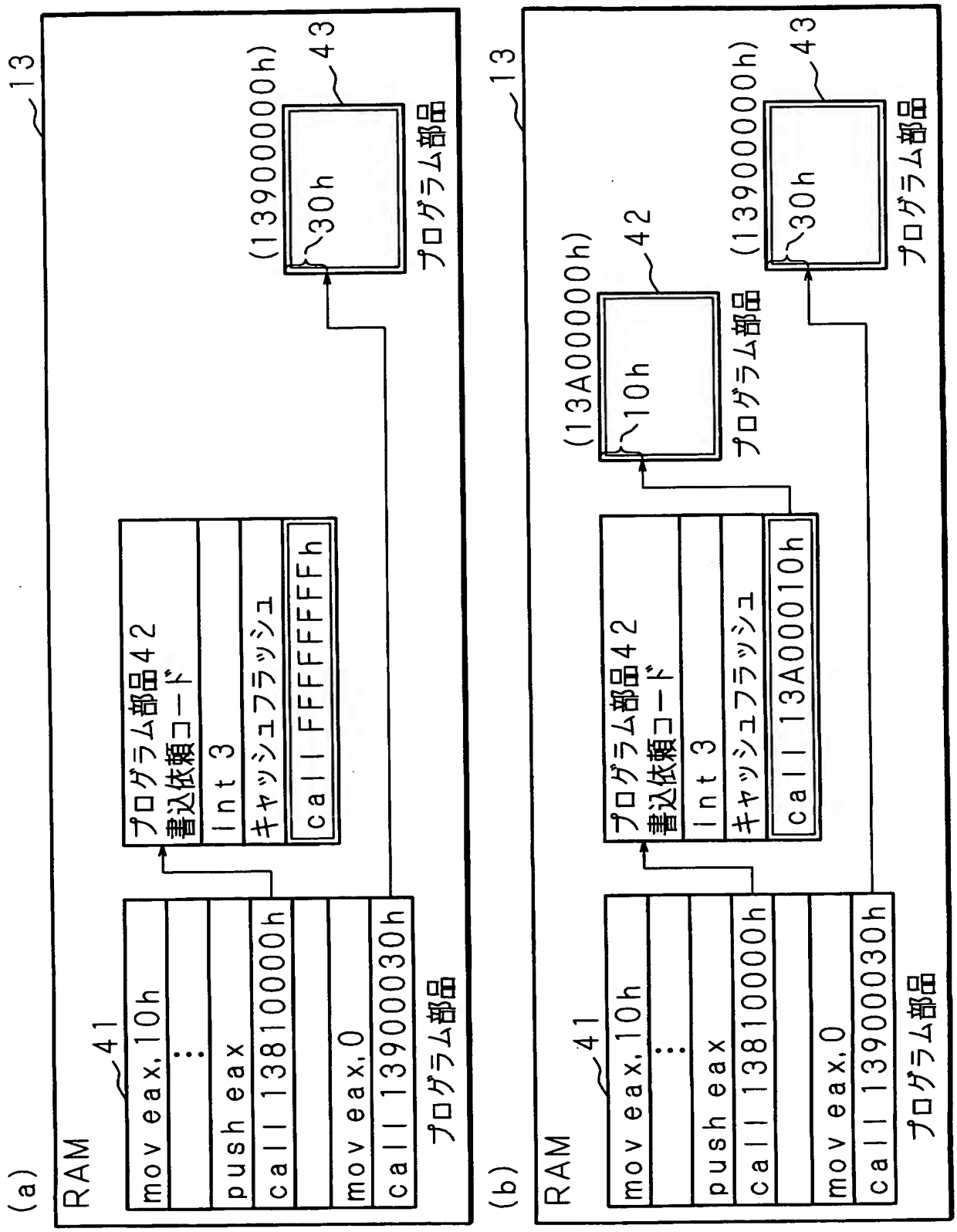
【図１３】

プログラム部品の動的書き込み処理及びリンク処理についての説明図



【図１４】

プログラム部品の動的書き込み処理及びリンク処理についての説明図



【書類名】要約書
【要約】
【課題】　プログラムを実行する場合に、悪意ある第三者による逆解析を困難にし、実行するロードモジュールの安全性を高めることができる情報処理装置を提供する。
【解決手段】　第１の記憶手段13と、該第１の記憶手段13に書き込まれたプログラムを実行するＣＰＵと、セキュアモジュール20と、暗号化されたプログラムを記憶する第２の記憶手段とを有する情報処理装置において、第２の記憶手段は、複数に分割されたプログラムを記憶してあり、ＣＰＵは、第２の記憶手段に記憶されたプログラムをセキュアモジュール20へ転送すべくなしてあり、セキュアモジュール20は、第２の記憶手段に記憶されたプログラムを受け取る手段と、受け取ったプログラムを実行可能な状態へ復帰させる手段と、ＣＰＵが実行する順序で、実行可能な状態へ復帰されたプログラムを第１の記憶手段13に書き込む手段と、ＣＰＵにより実行終了後に第１の記憶手段13から削除する手段とを備える。
【選択図】　図５

特願２００３－３７２３７４

出願人履歴情報

識別番号　［０００００５２２３］

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社